⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　昭60－62252

⑤1Int.Cl.⁴	識別記号	庁内整理番号	㊸公開　昭和60年(1985)4月10日
H 04 L 9/02		7240－5K	
G 06 K 19/00		6711－5B	
G 09 C 1/00		7368－5B	審査請求　有　発明の数 1　（全3頁）

㊹発明の名称　暗号回路内蔵カード

㉑特　願　昭58－169242

㉒出　願　昭58(1983)9月16日

㉒発明者　内平　直志　川崎市幸区小向東芝町1　東京芝浦電気株式会社総合研究所内

㉑出願人　株式会社東芝　川崎市幸区堀川町72番地

㉔代理人　弁理士　則近　憲佑　外1名

明　細　書

1. 発明の名称

暗号回路内蔵カード

2. 特許請求の範囲

(1)予め登録されたカード固有番号を記憶しておく記憶媒体と、この記憶媒体から出力されたカード固有番号と外部から入力された乱数を用いてキーコードを発生する演算回路と、この演算回路から出力されたキーコードを用いて送信すべきデータを暗号化して出力する暗号化回路とを具備したことを特徴とする暗号回路内蔵カード。

(2)送信すべきデータは外部から暗号回路へ入力されることを特徴とする特許請求の範囲第1項記載の暗号回路内蔵カード。

(3)送信すべきデータは記憶媒体に予め記憶されていることを特徴とする特許請求の範囲第1項記載の暗号回路内蔵カード。

3. 発明の詳細な説明

〔発明の技術分野〕

本発明は通信における送信内容の漏洩、偽造を防ぐための暗号回路内蔵カードに関する。

〔発明の技術的背景とその問題点〕

近年、演算機能と記憶機能を合わせ持つICカードを用いて情報（原データ）を他へ送信する場合、この送信内容の盗聴、悪意による変更を防ぐ必要のある場合が生じる。従来は、このような目的から、外から与えられる乱数に応じてICカードが発生するキーコード（暗号キー）を用いて、外部の暗号化装置が原データを暗号化して送信している。

ところがこの方式では、暗号キーが暗号化装置に送信される間に一端外部に出るため、そこでの何らかの悪意を持った操作が可能である。例えばICカードから暗号化回路へ送信された暗号キー、及び暗号化回路より送信された暗号化されたデータを外部の者が取り出し、市販されている暗号解読回路を使って原データを盗むことが可能である。又、原データが記憶媒体に記憶されているICカードにおいては、このカードの所有者が自己の原データが暗号化回路へ送信される接続線をカット

し、他の偽造データを送信することも可能である。このように従来のＩＣカードにおいては送信内容の漏洩・偽造の危険性を伴うものであった。

〔発明の目的〕

本発明の目的は、暗号キーがカードの外部に出ることなく漏洩・偽造の発生を防ぐカードを提供することにある。

〔発明の概要〕

本発明はカード内において、記憶媒体に記憶されたカード固有番号と外部から入力された乱数とから演算回路で暗号化のキーコードを生成し、暗号化回路では演算回路で作られたキーコードを用いて送信すべきデータを暗号化して出力するものである。

〔発明の効果〕

本発明によれば、暗号化のキーコードは一切外部には漏れずに暗号化された信号だけが外部に出るので、暗号信号を解読・偽造することが出来なくなり、情報の漏洩を防ぐ意味で実用的利点が増大する。

〔発明の実施例〕

以下、本発明の一実施例につき図面を参照して説明する。

第１図は本実施例の概要を示す図である。サービスを受ける端末（以下サービス端末という）１は、サービスを管理するセンタ（以下サービスセンタという）３と信号伝送路２で結ばれている。サービスの受けられる範囲に関する個別な情報は、サービス端末１の中に存在するが、その情報は本発明によるカードにより直接外部に出ることなく暗号化されてサービスセンタ３に送られる。サービスセンタ３ではその暗号を後に述べる方式で解読し、サービス端末１から送られてくるサービス要請に対し、そのサービス要請がサービス範囲内のものかを判断し、サービスを実行するかしないかの判断を下す。

第２図は本発明の一実施例によるカードを示す図である。カード11はこのカード固有の番号を記憶させた記憶媒体12とキーコードを計算する演算回路13と暗号化を行なう暗号化回路14と信号伝送路15,16,17,18,19から構成される。まず、外部から伝送路16を通して乱数Ｒを入力し、この乱数Ｒと記憶媒体12のカード固有番号Ｉから演算回路13で暗号化のキーコードＫを生成して暗号化回路14に送る。暗号化回路14は外部からの送信すべき原データを伝送路18から入力し、キーコードを基に暗号化し伝送路19を通して出力する。この装置はカード11内に一体化されていて、外部からは一切中の状態がわからないように作られる。この第２図の実施例によれば暗号化回路14がカード11に内蔵されているので、キーコードが外部に出る事が無くなり原データの漏洩を防げる。

第３図は本発明の他の実施例であり、サービス端末側に組み込まれるサービスカード20の概略構成図である。サービスカード20は第２図のカードの信号伝送路18を通して入力するデータをカード内部の記憶媒体21の記憶内容として組み込んだものであり、この記憶媒体21にはサービス範囲に関する情報Ｓが記憶されている。このサービス範囲情報Ｓとは例えば銀行システムに応用した場合の預金高、借入限度額等にあたる。記憶媒体22に記憶されているカード固有の符号Ｉと信号伝送路23から送られてくる乱数Ｒから、演算回路24が外部には漏れないある計算規則Ｋ＝Ｐ(Ｉ,Ｒ)により暗号キーコードＫを計算する。暗号キーコードＫを基に、サービス範囲の情報Ｓを暗号化回路25で暗号化し、信号伝送路26を通して外部に伝送する。（尚、記憶媒体21と記憶媒体22は一体化されていてもよい。）

第４図は第１図を詳細化したもので第３図の実施例が一部として組み込まれている。先ずカード所有者はサービス端末１にサービスカード20をセットした後信号伝送路27を通してサービスセンタ３にサービスカード20の識別コード（たとえばＣＤカードの場合は暗証番号）を送る。するとコントローラ28がサービスカード20のマスターカード29を選択する。（サービスセンタ側にはカード所有者全てのマスターカードがある。）マスターカード29はサービスカード20から暗号化回路25と記憶媒体21を除いたもので記憶媒体22と記憶媒体30には同一

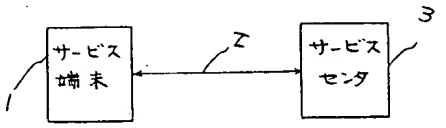
のカード固有番号Iが記憶されており、演算回路24と演算回路31も同じものである。このときコントローラ28から乱数Rが信号伝送路23，32を通してサービスカード20とマスターカード29に同時に送られる。すると演算回路24と演算回路31では計算規則K=P(I,R)により同じ暗号キーコードKが発生される。サービスカード20では記憶媒体21の内容であるサービス範囲の情報Sを暗号キーコードKを基に暗号化回路25で暗号化し信号伝送路26を通してサービスセンタ3に送る。サービスセンタ3では暗号解読回路33において、マスターカード29から得られた暗号キーコードKを基に暗号を解読し、サービス範囲情報Sを復元することができる。そしてSを記憶媒体34に記憶させる。それ以後、サービス端末1からサービス要請（例えば現金引き出し）があった場合、コントローラ28が記憶媒体34のサービス範囲情報S（預金高）と照らし合わせてそのサービスを実行するかしないかの判断を下す。この実施例によれば暗号化回路25ばかりでなく記憶媒体21もサービスカード20に内蔵されているので、カード所有者が他のデータを暗号化回路へ送信することが不可能となり偽造を防げる。又、従来サービスセンタのデータベースに蓄えられていたサービス範囲情報を、各サービスカードの内部に分散させて記憶させることが出来るのでサービスセンタのデータ記憶領域を大幅に軽減することができる。

4. 図面の簡単な説明

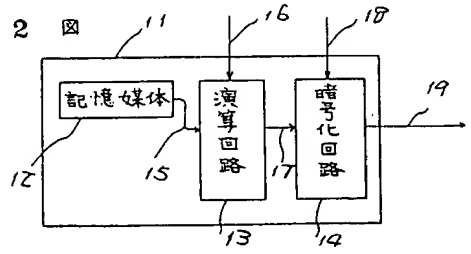
第1図は本発明の実施例の概要を示す図、第2図は本発明の一実施例によるカードを示す図、第3図は本発明の他の実施例のカードを示す図、第4図は第3図の実施例が組み込まれた第1図を詳細化した図である。

1…サービス端末、2…信号伝送路、3…サービスセンタ、11…カード、12,21,22,30,34…記憶媒体、13,24,31…演算回路、14,25…暗号化回路、15,16,17,18,19,23,26,27,32…信号伝送路、20…サービスカード、28…コントローラ、29…マスターカード、33…暗号解読回路。

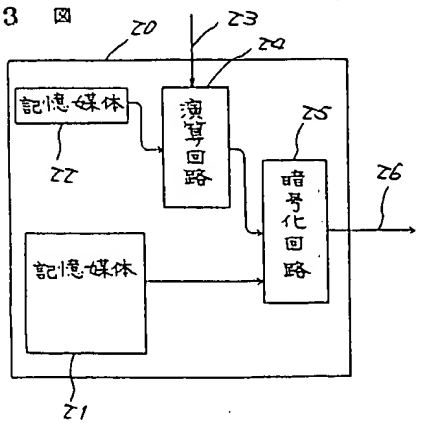
第1図



第2図



第3図



第4図